FIG. 1 (PRIOR ART)

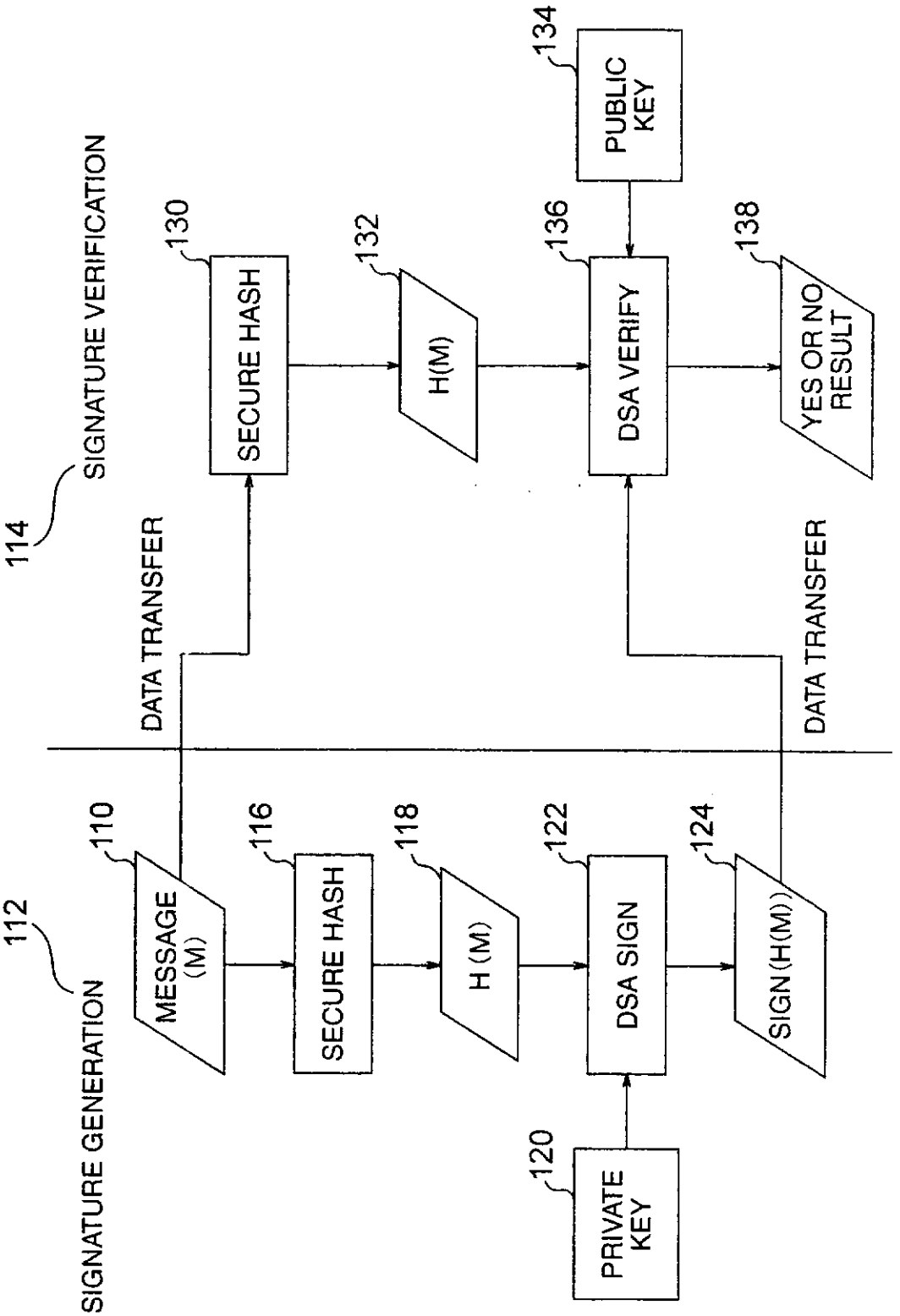


FIG. 2

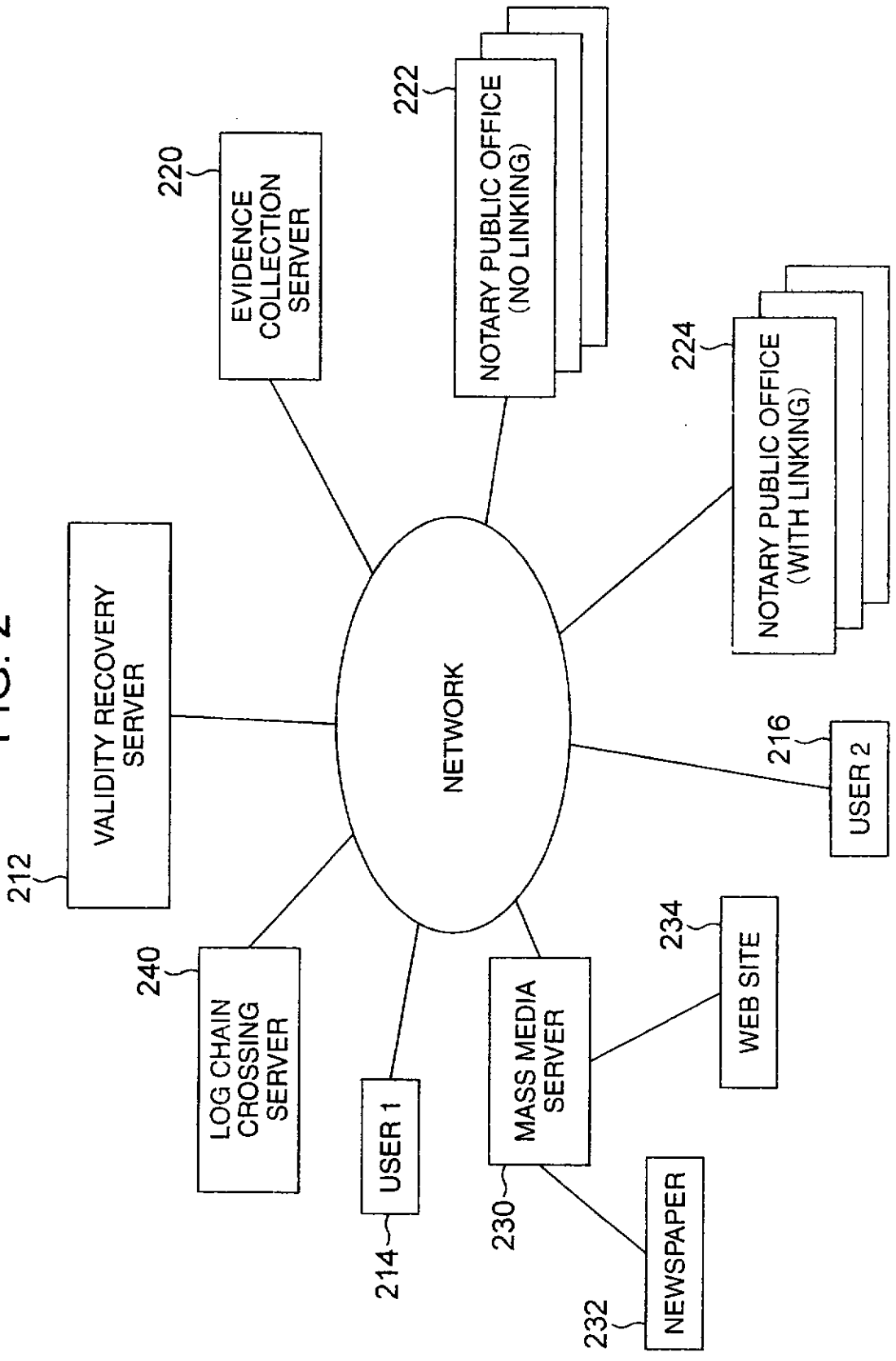

NETWORK
VALIDITY RECOVERY SERVER
212
EVIDENCE COLLECTION SERVER
220
NOTARY PUBLIC OFFICE (NO LINKING)
222
NOTARY PUBLIC OFFICE (WITH LINKING)
224
USER 2
216
LOG CHAIN CROSSING SERVER
240
USER 1
214
MASS MEDIA SERVER
230
WEB SITE
234
NEWSPAPER
232

FIG. 3

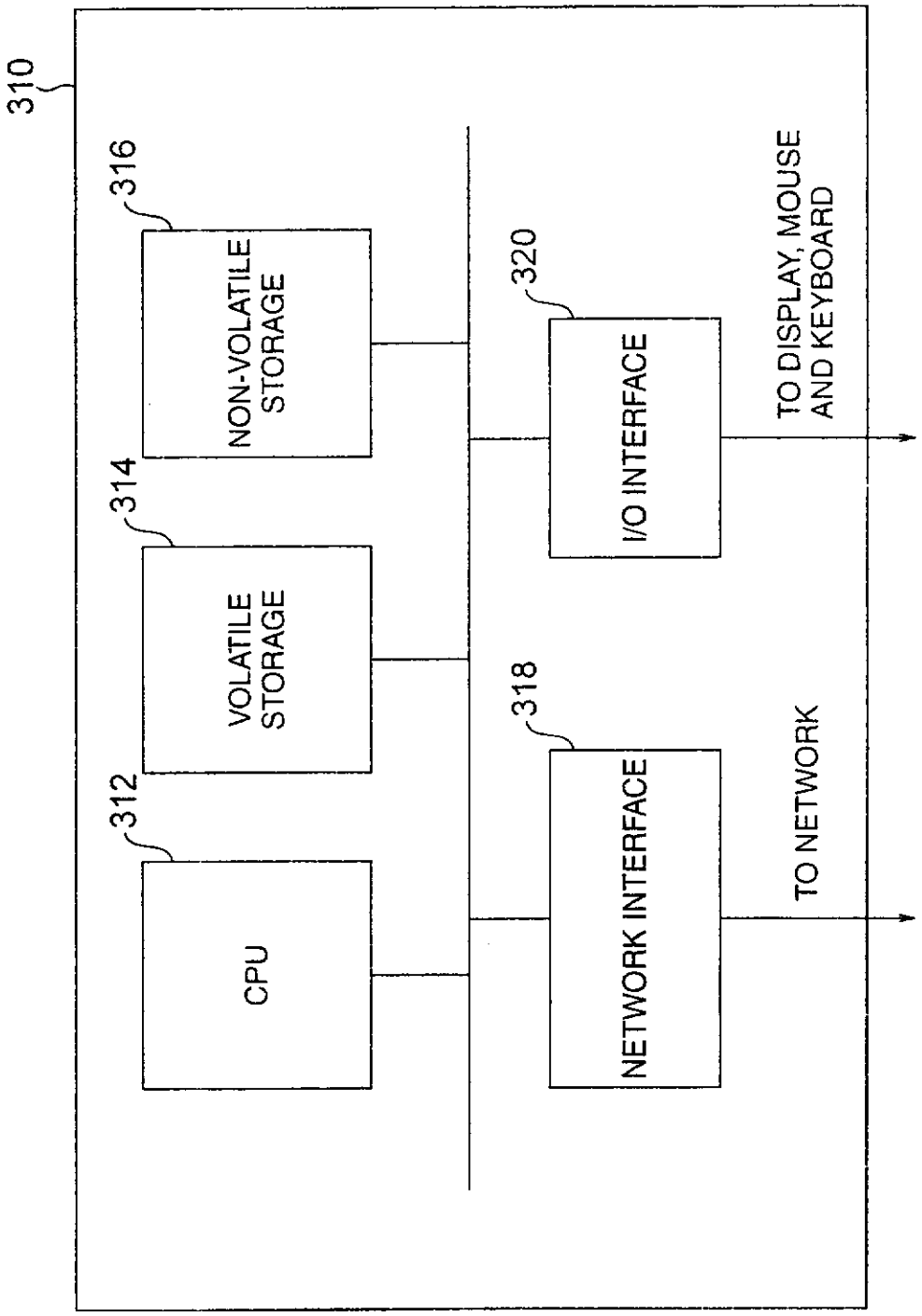

310
316
NON-VOLATILE STORAGE
314
VOLATILE STORAGE
312
CPU
320
I/O INTERFACE
TO DISPLAY, MOUSE AND KEYBOARD
318
NETWORK INTERFACE
TO NETWORK

FIG. 4

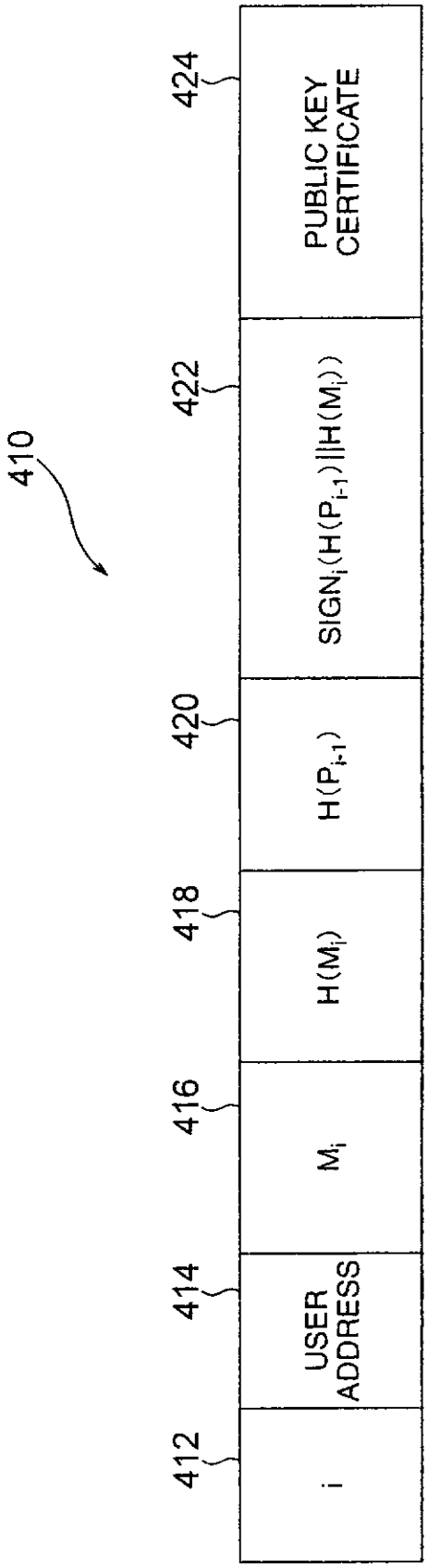

410
412
i
414
USER ADDRESS
416
M_i
418
$H(M_i)$
420
$H(P_{i-1})$
422
$SIGN_i(H(P_{i-1})||H(M_i))$
424
PUBLIC KEY CERTIFICATE

FIG. 5

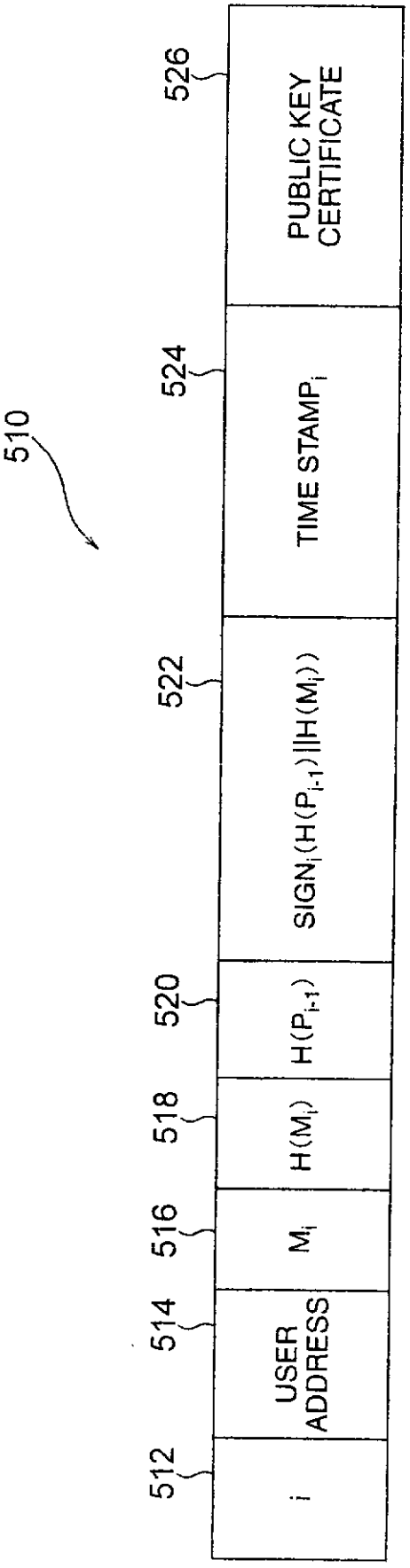

510
512
i
514
USER ADDRESS
516
M_i
518
$H(M_i)$
520
$H(P_{i-1})$
522
$SIGN_i(H(P_{i-1})||H(M_i))$
524
$TIME\ STAMP_i$
526
PUBLIC KEY CERTIFICATE

FIG. 6

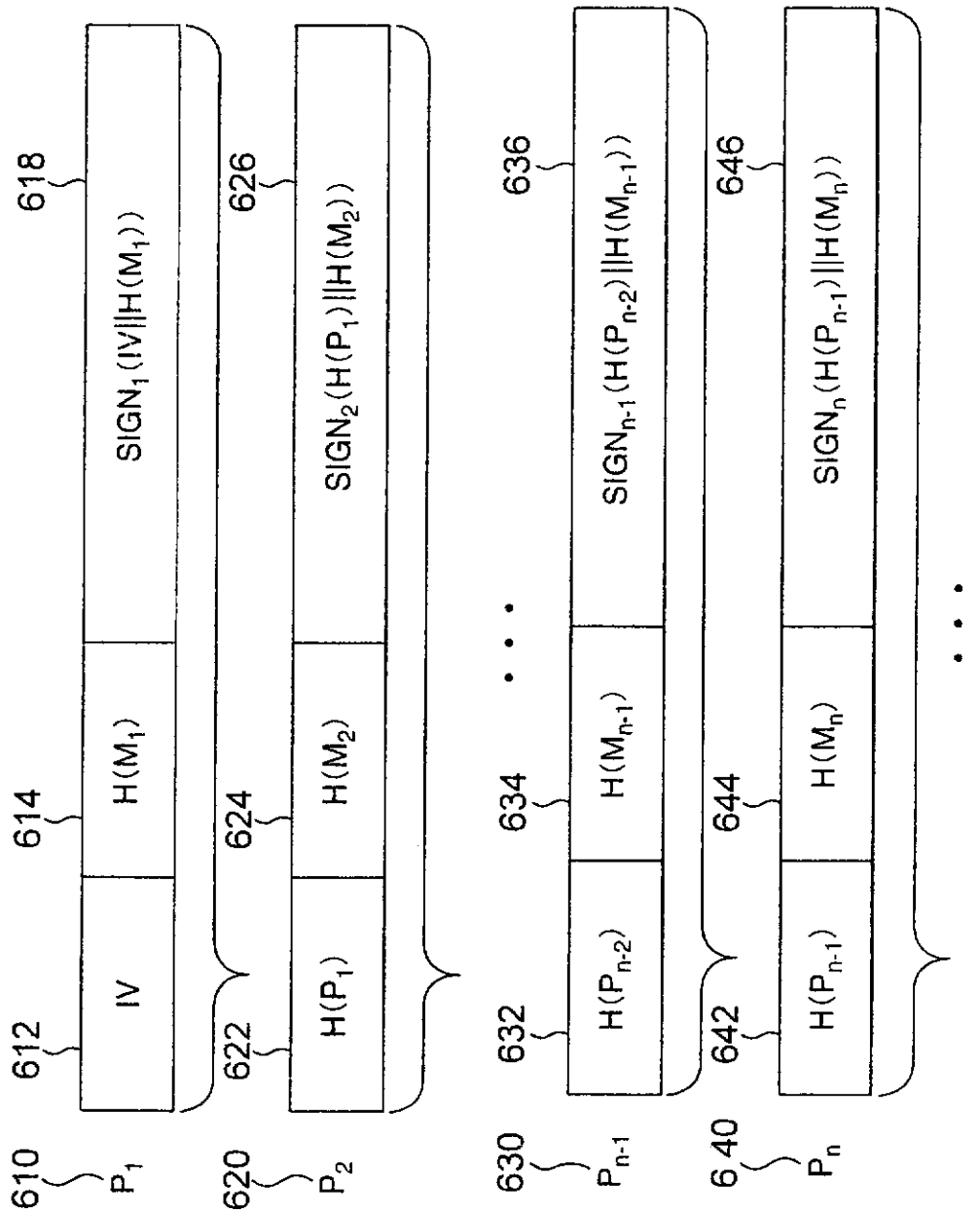

610
P_1
612
IV
614
$H(M_1)$
618
$SIGN_1(IV||H(M_1))$
620
P_2
622
$H(P_1)$
624
$H(M_2)$
626
$SIGN_2(H(P_1)||H(M_2))$
630
P_{n-1}
632
$H(P_{n-2})$
634
$H(M_{n-1})$
636
$SIGN_{n-1}(H(P_{n-2})||H(M_{n-1}))$
640
P_n
642
$H(P_{n-1})$
644
$H(M_n)$
646
$SIGN_n(H(P_{n-1})||H(M_n))$

FIG. 7

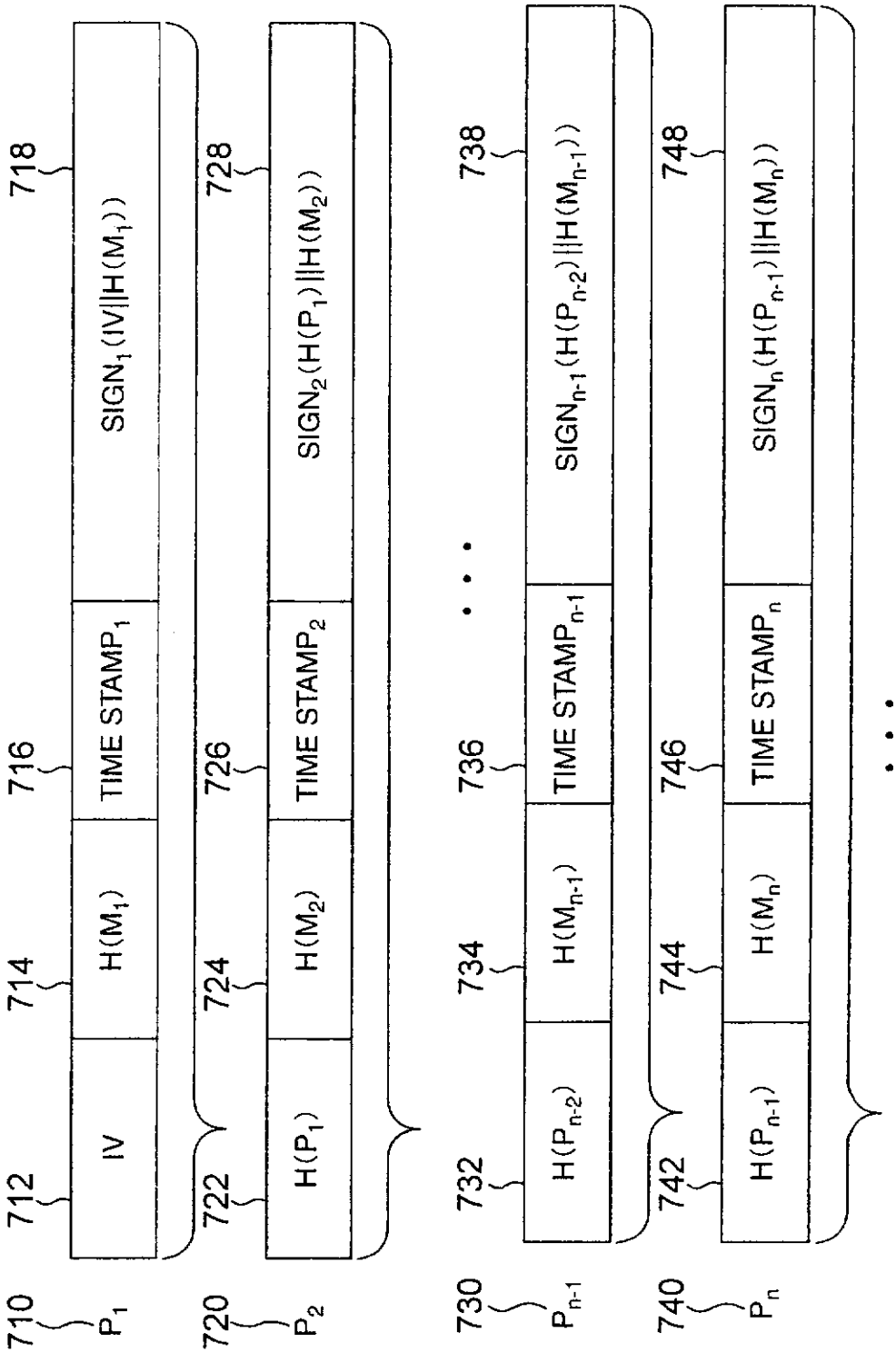

710
P_1
712
IV
714
$H(M_1)$
716
TIME STAMP$_1$
718
SIGN$_1$ (IV||$H(M_1)$)
720
P_2
722
$H(P_1)$
724
$H(M_2)$
726
TIME STAMP$_2$
728
SIGN$_2$($H(P_1)$||$H(M_2)$)
730
P_{n-1}
732
$H(P_{n-2})$
734
$H(M_{n-1})$
736
TIME STAMP$_{n-1}$
738
SIGN$_{n-1}$($H(P_{n-2})$||$H(M_{n-1})$)
740
P_n
742
$H(P_{n-1})$
744
$H(M_n)$
746
TIME STAMP$_n$
748
SIGN$_n$($H(P_{n-1})$||$H(M_n)$)

FIG. 8

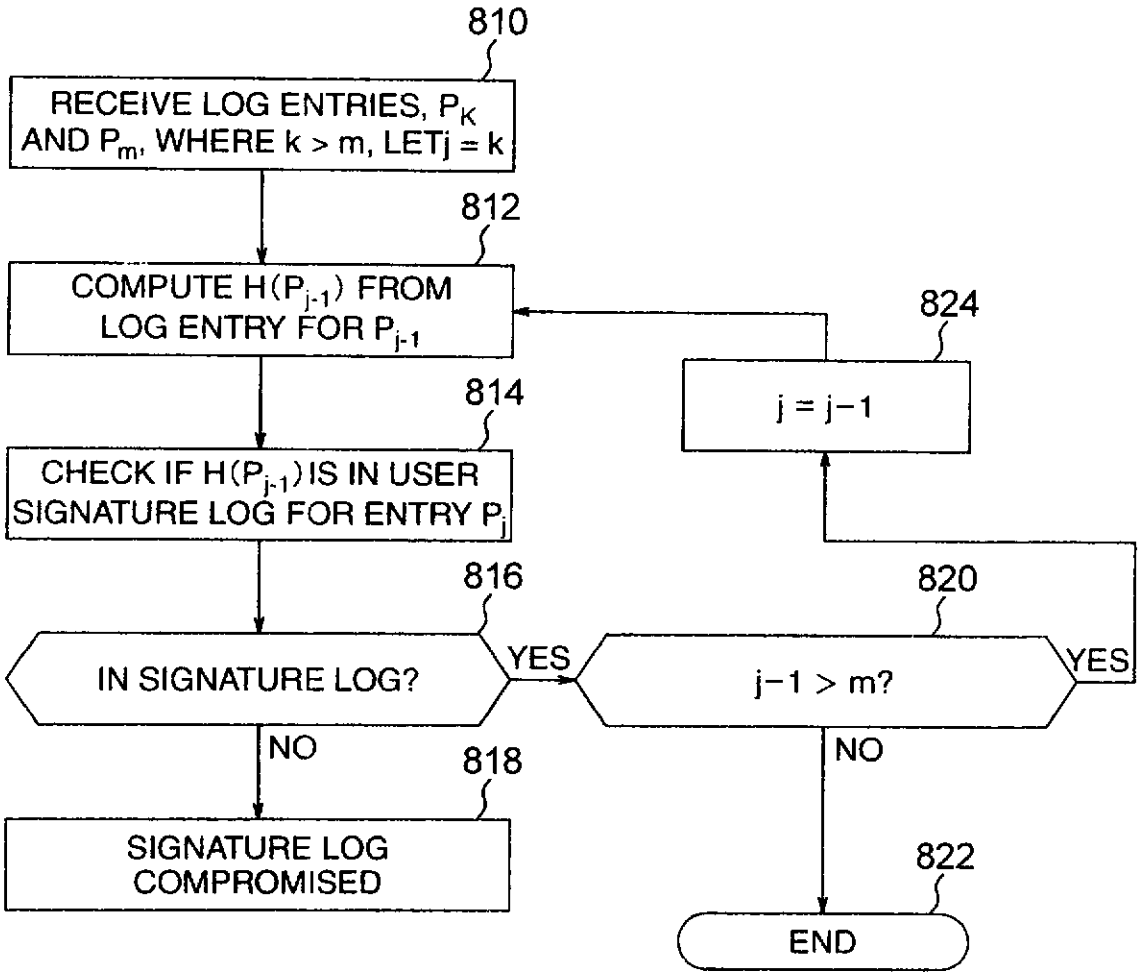

810
RECEIVE LOG ENTRIES, P_K AND P_m, WHERE k > m, LETj = k
812
COMPUTE $H(P_{j-1})$ FROM LOG ENTRY FOR P_{j-1}
814
CHECK IF $H(P_{j-1})$ IS IN USER SIGNATURE LOG FOR ENTRY P_j
816
IN SIGNATURE LOG?
YES
NO
818
SIGNATURE LOG COMPROMISED
820
j−1 > m?
YES
NO
824
j = j−1
822
END

FIG. 9

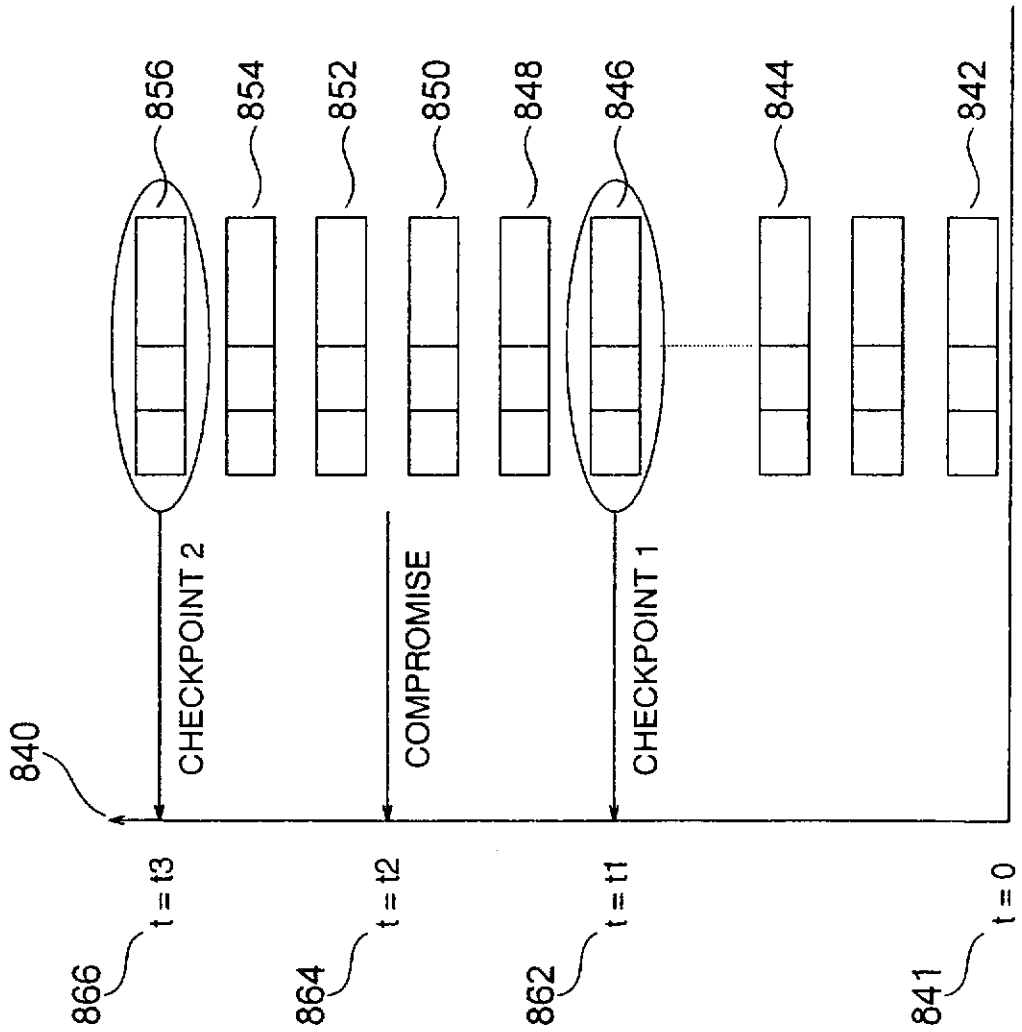

856
854
852
850
848
846
844
842
840
CHECKPOINT 2
COMPROMISE
CHECKPOINT 1
t = t3
t = t2
t = t1
t = 0
866
864
862
841

FIG. 10

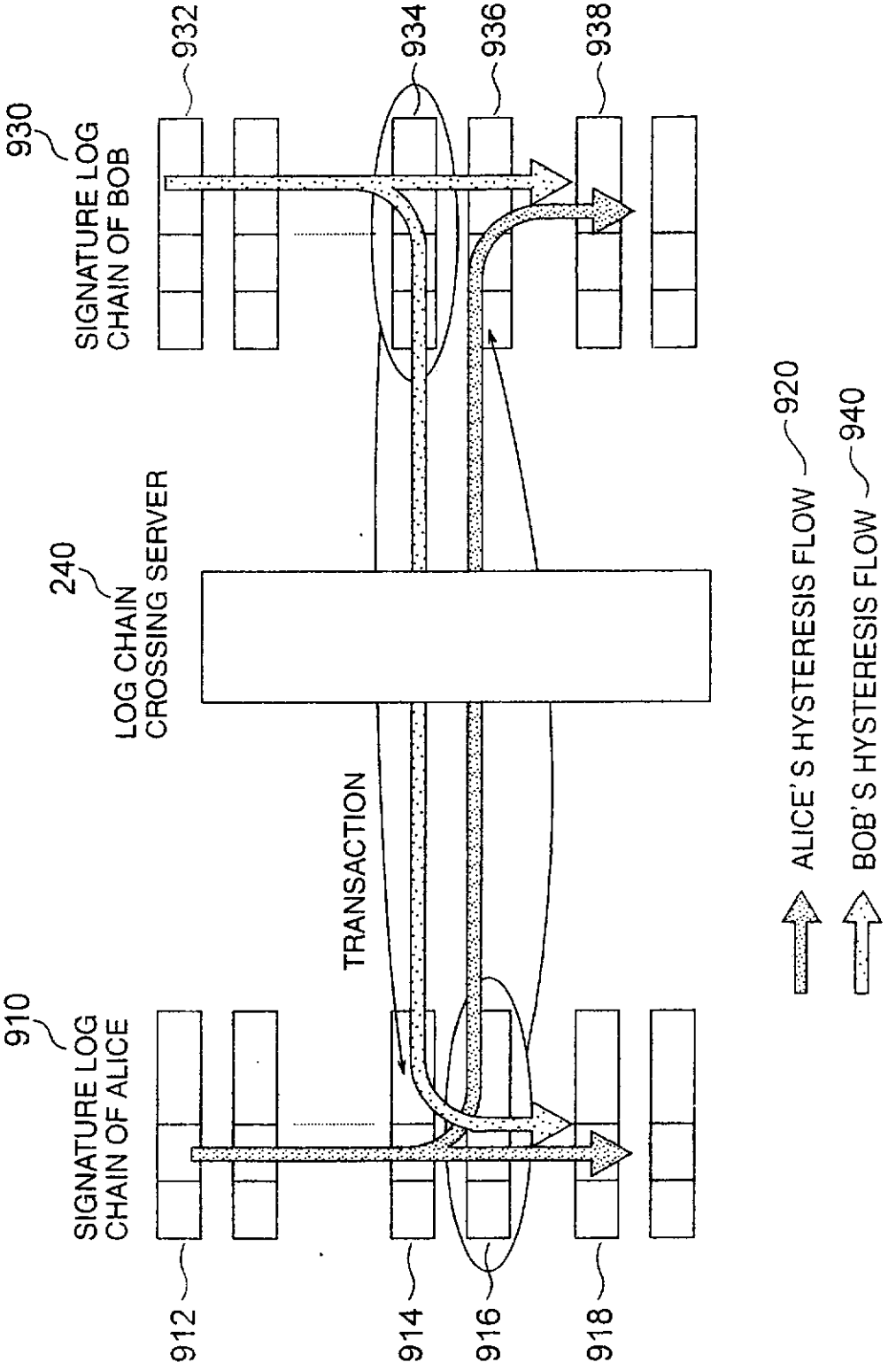

930
SIGNATURE LOG CHAIN OF BOB
932
934
936
938
240
LOG CHAIN CROSSING SERVER
TRANSACTION
910
SIGNATURE LOG CHAIN OF ALICE
912
914
916
918
920
ALICE'S HYSTERESIS FLOW
940
BOB'S HYSTERESIS FLOW

FIG. 11

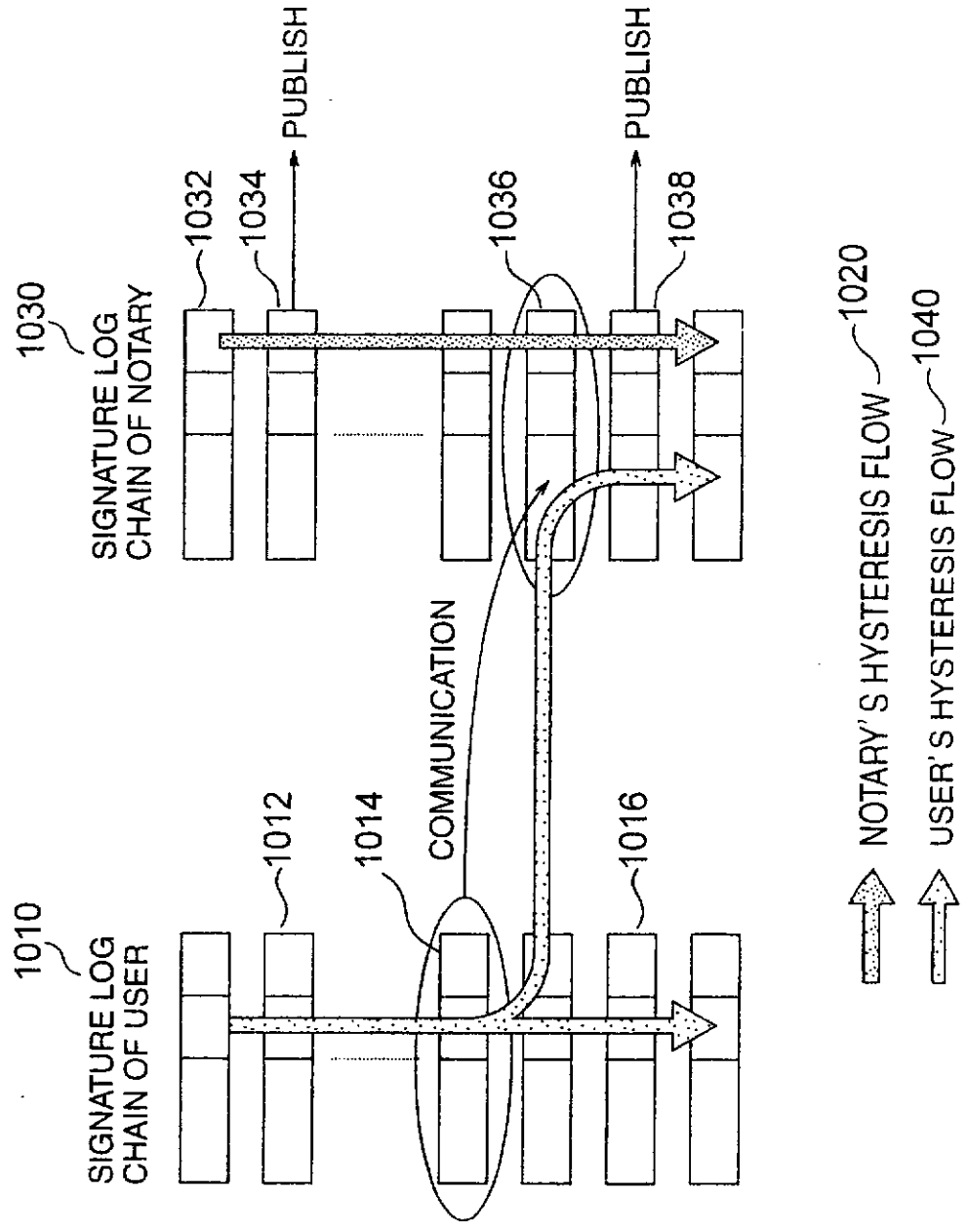

1030
SIGNATURE LOG CHAIN OF NOTARY
1032
1034
PUBLISH
1036
PUBLISH
1038
1010
SIGNATURE LOG CHAIN OF USER
1012
1014
COMMUNICATION
1016
1020
NOTARY'S HYSTERESIS FLOW
1040
USER'S HYSTERESIS FLOW

FIG. 12

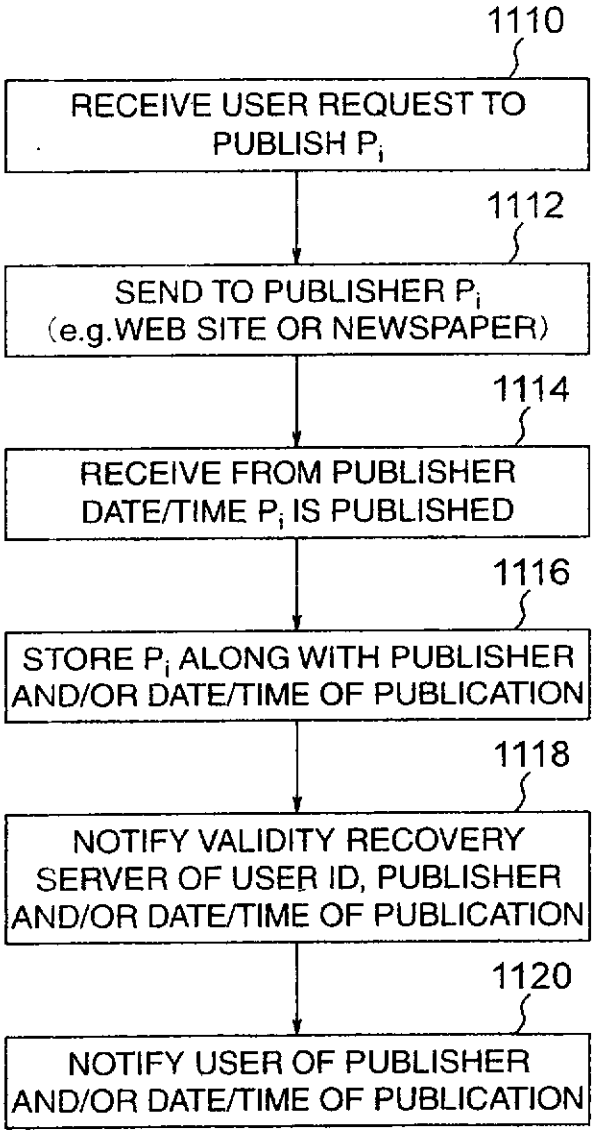

1110
RECEIVE USER REQUEST TO PUBLISH P_i
1112
SEND TO PUBLISHER P_i (e.g.WEB SITE OR NEWSPAPER)
1114
RECEIVE FROM PUBLISHER DATE/TIME P_i IS PUBLISHED
1116
STORE P_i ALONG WITH PUBLISHER AND/OR DATE/TIME OF PUBLICATION
1118
NOTIFY VALIDITY RECOVERY SERVER OF USER ID, PUBLISHER AND/OR DATE/TIME OF PUBLICATION
1120
NOTIFY USER OF PUBLISHER AND/OR DATE/TIME OF PUBLICATION

FIG. 13

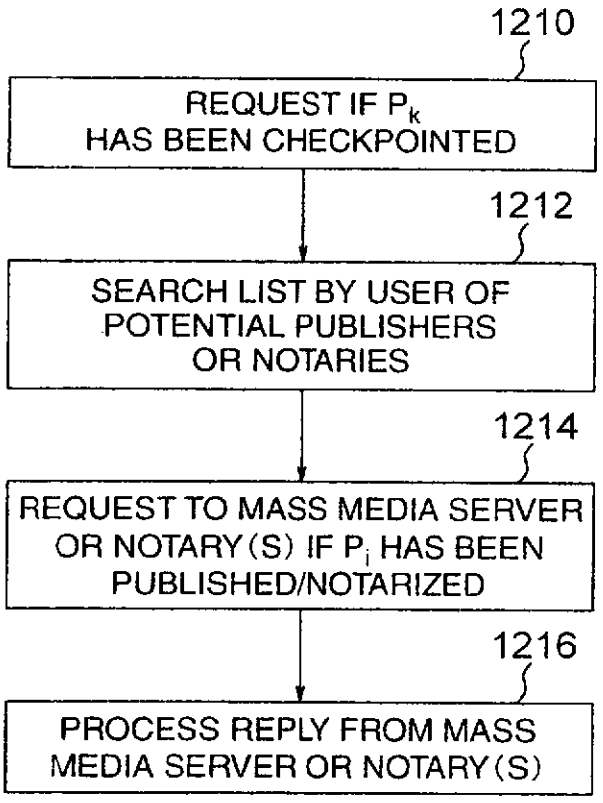

1210
REQUEST IF P_k HAS BEEN CHECKPOINTED
1212
SEARCH LIST BY USER OF POTENTIAL PUBLISHERS OR NOTARIES
1214
REQUEST TO MASS MEDIA SERVER OR NOTARY(S) IF P_i HAS BEEN PUBLISHED/NOTARIZED
1216
PROCESS REPLY FROM MASS MEDIA SERVER OR NOTARY(S)

FIG. 14

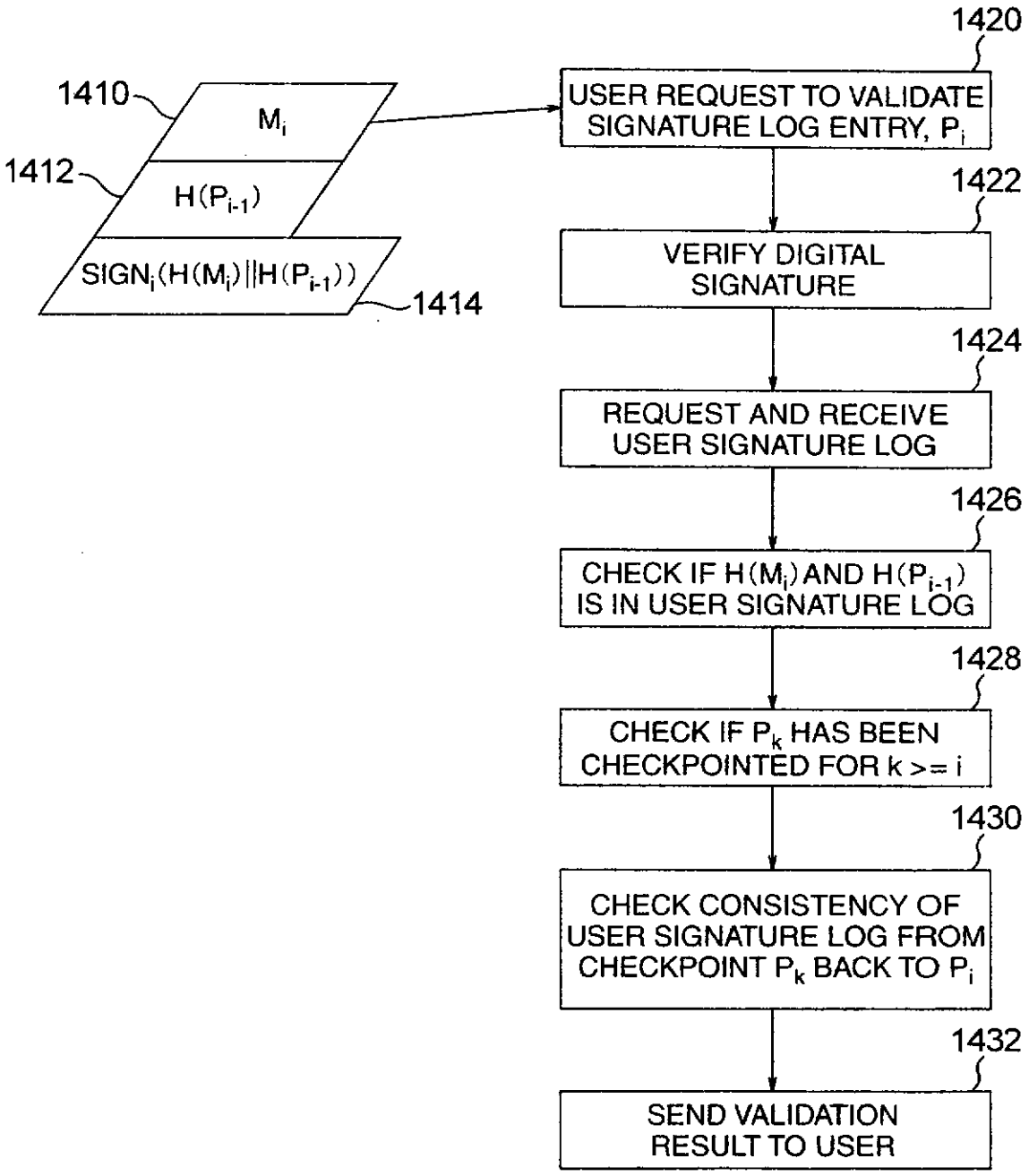

1420
USER REQUEST TO VALIDATE SIGNATURE LOG ENTRY, P_i
1410
M_i
1412
$H(P_{i-1})$
$SIGN_i(H(M_i)||H(P_{i-1}))$
1414
1422
VERIFY DIGITAL SIGNATURE
1424
REQUEST AND RECEIVE USER SIGNATURE LOG
1426
CHECK IF $H(M_i)$ AND $H(P_{i-1})$ IS IN USER SIGNATURE LOG
1428
CHECK IF P_k HAS BEEN CHECKPOINTED FOR $k >= i$
1430
CHECK CONSISTENCY OF USER SIGNATURE LOG FROM CHECKPOINT P_k BACK TO P_i
1432
SEND VALIDATION RESULT TO USER

FIG. 15

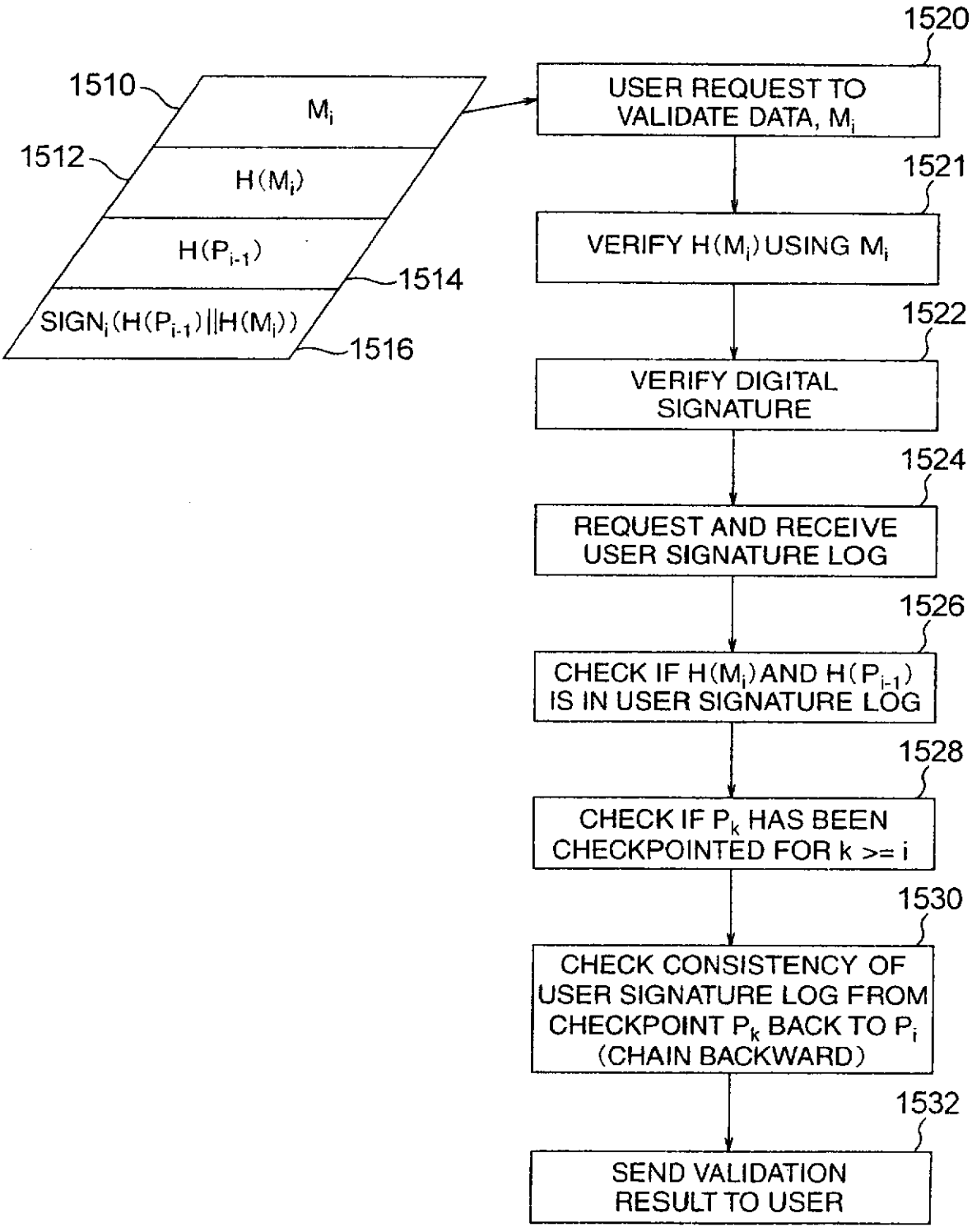

1510
M_i
1512
$H(M_i)$
$H(P_{i-1})$
1514
$SIGN_i(H(P_{i-1})||H(M_i))$
1516
1520
USER REQUEST TO VALIDATE DATA, M_i
1521
VERIFY $H(M_i)$ USING M_i
1522
VERIFY DIGITAL SIGNATURE
1524
REQUEST AND RECEIVE USER SIGNATURE LOG
1526
CHECK IF $H(M_i)$ AND $H(P_{i-1})$ IS IN USER SIGNATURE LOG
1528
CHECK IF P_k HAS BEEN CHECKPOINTED FOR k >= i
1530
CHECK CONSISTENCY OF USER SIGNATURE LOG FROM CHECKPOINT P_k BACK TO P_i (CHAIN BACKWARD)
1532
SEND VALIDATION RESULT TO USER

FIG. 16

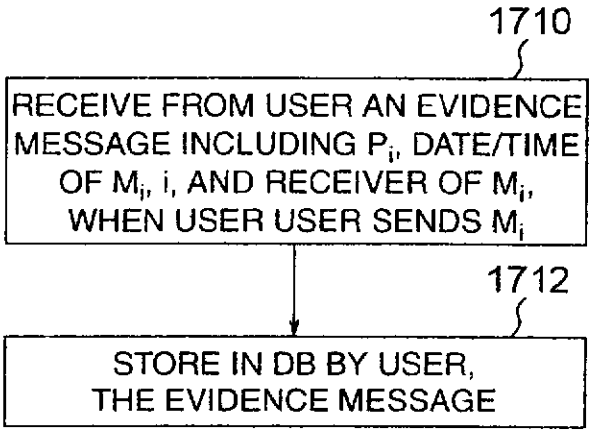

1710
RECEIVE FROM USER AN EVIDENCE MESSAGE INCLUDING P_i, DATE/TIME OF M_i, i, AND RECEIVER OF M_i, WHEN USER USER SENDS M_i
1712
STORE IN DB BY USER, THE EVIDENCE MESSAGE

FIG. 17

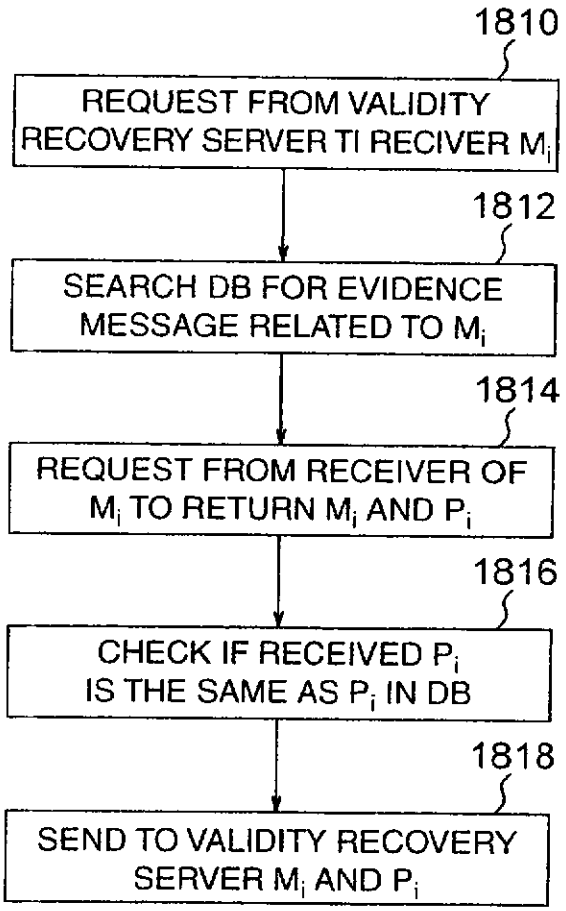

1810
REQUEST FROM VALIDITY RECOVERY SERVER TI RECIVER M_i
1812
SEARCH DB FOR EVIDENCE MESSAGE RELATED TO M_i
1814
REQUEST FROM RECEIVER OF M_i TO RETURN M_i AND P_i
1816
CHECK IF RECEIVED P_i IS THE SAME AS P_i IN DB
1818
SEND TO VALIDITY RECOVERY SERVER M_i AND P_i

FIG. 18

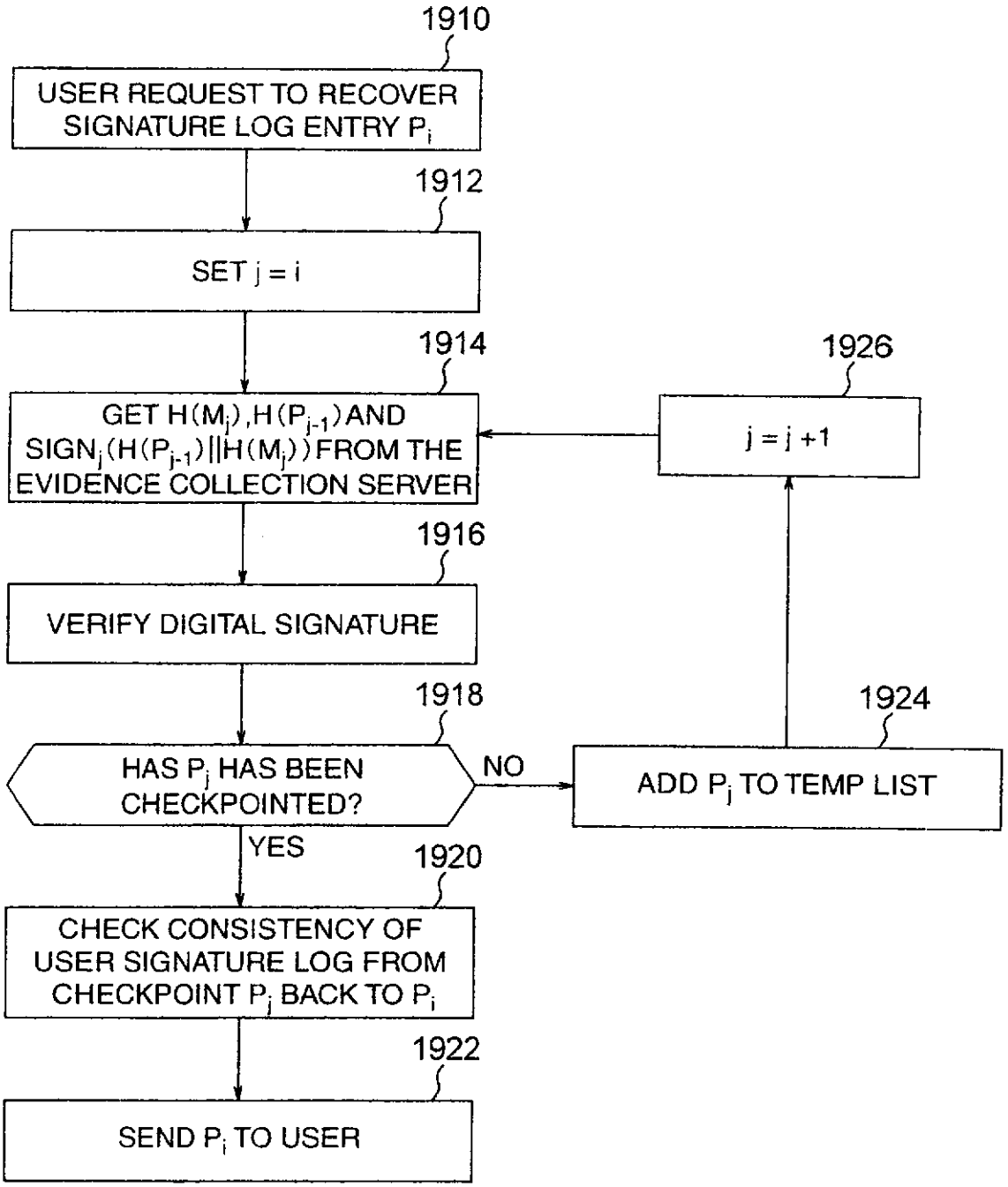

1910
USER REQUEST TO RECOVER SIGNATURE LOG ENTRY P_i
1912
SET j = i
1914
GET $H(M_j)$, $H(P_{j-1})$ AND $SIGN_j(H(P_{j-1})||H(M_j))$ FROM THE EVIDENCE COLLECTION SERVER
1916
VERIFY DIGITAL SIGNATURE
1918
HAS P_j HAS BEEN CHECKPOINTED?
NO
YES
1920
CHECK CONSISTENCY OF USER SIGNATURE LOG FROM CHECKPOINT P_j BACK TO P_i
1922
SEND P_i TO USER
1924
ADD P_j TO TEMP LIST
1926
j = j +1

FIG. 19

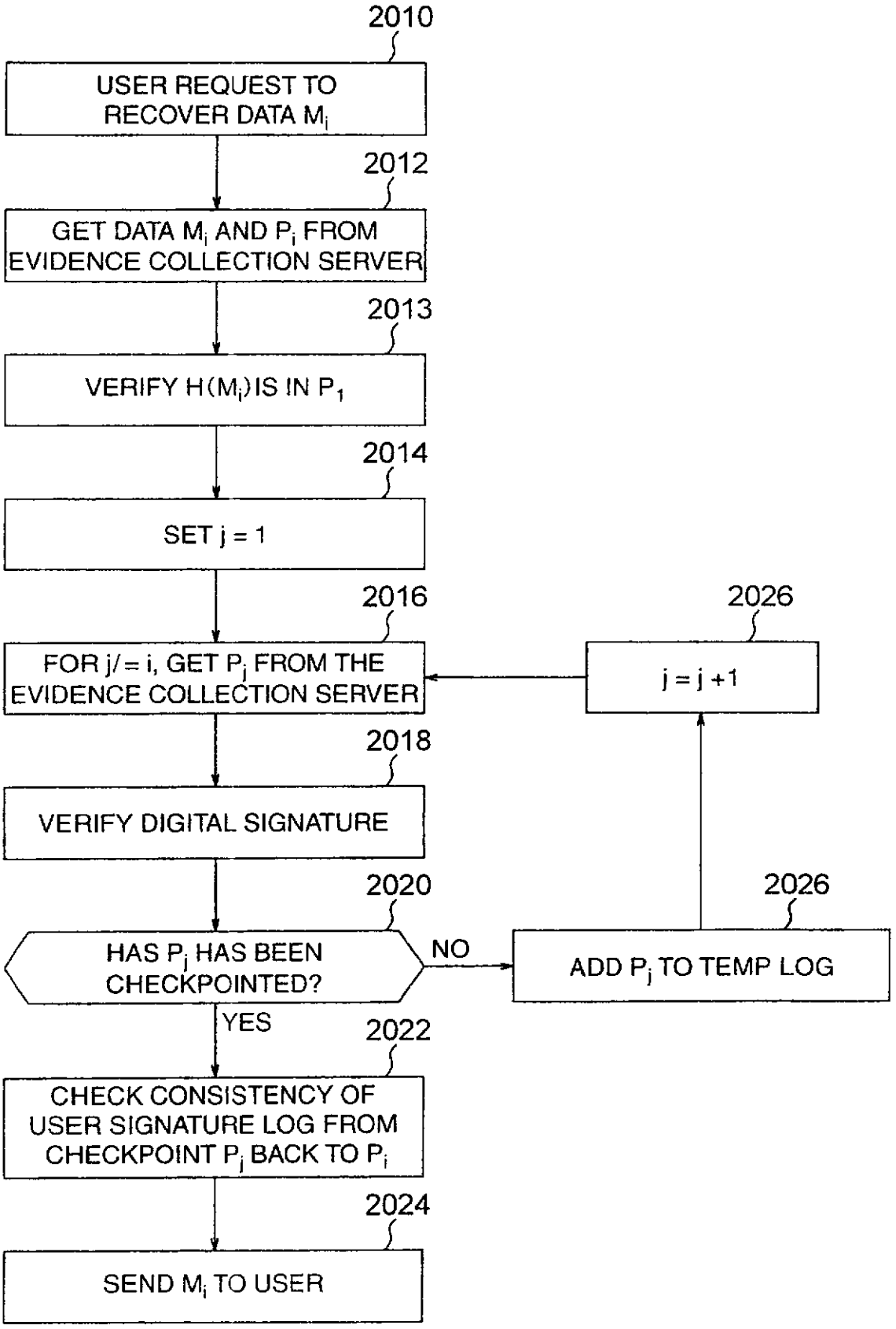
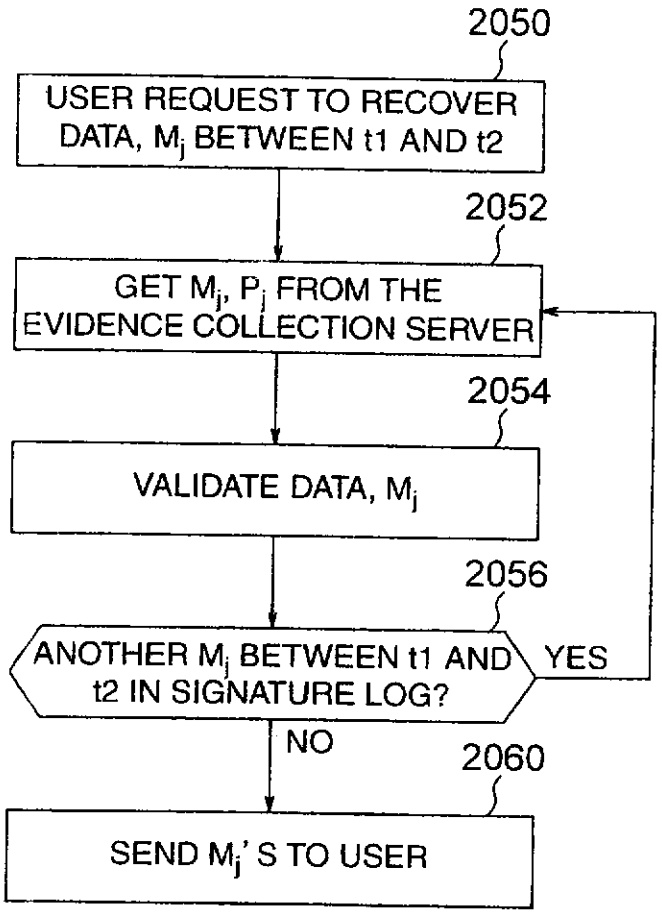

2010
USER REQUEST TO RECOVER DATA M_i
2012
GET DATA M_i AND P_i FROM EVIDENCE COLLECTION SERVER
2013
VERIFY $H(M_i)$ IS IN P_1
2014
SET j = 1
2016
FOR j/= i, GET P_j FROM THE EVIDENCE COLLECTION SERVER
2026
j = j +1
2018
VERIFY DIGITAL SIGNATURE
2020
HAS P_j HAS BEEN CHECKPOINTED?
NO
2026
ADD P_j TO TEMP LOG
YES
2022
CHECK CONSISTENCY OF USER SIGNATURE LOG FROM CHECKPOINT P_j BACK TO P_i
2024
SEND M_i TO USER

FIG. 20


2050
USER REQUEST TO RECOVER DATA, M_j BETWEEN t1 AND t2
2052
GET M_j, P_j FROM THE EVIDENCE COLLECTION SERVER
2054
VALIDATE DATA, M_j
2056
ANOTHER M_j BETWEEN t1 AND t2 IN SIGNATURE LOG?
YES
NO
2060
SEND M_j' S TO USER